

# VoIP Wars: Destroying Jar Jar Lync

Fatih Ozavci

13 November 2015

Compliance, Protection & Business Confidence

## Sense of Security Pty Ltd

### **Sydney**

Level 8, 66 King Street  
Sydney NSW 2000 Australia

### **Melbourne**

Level 15, 401 Docklands Drv  
Docklands VIC 3008 Australia

T: 1300 922 923

T: +61 (0) 2 9290 4444  
F: +61 (0) 2 9290 4455

info@senseofsecurity.com.au

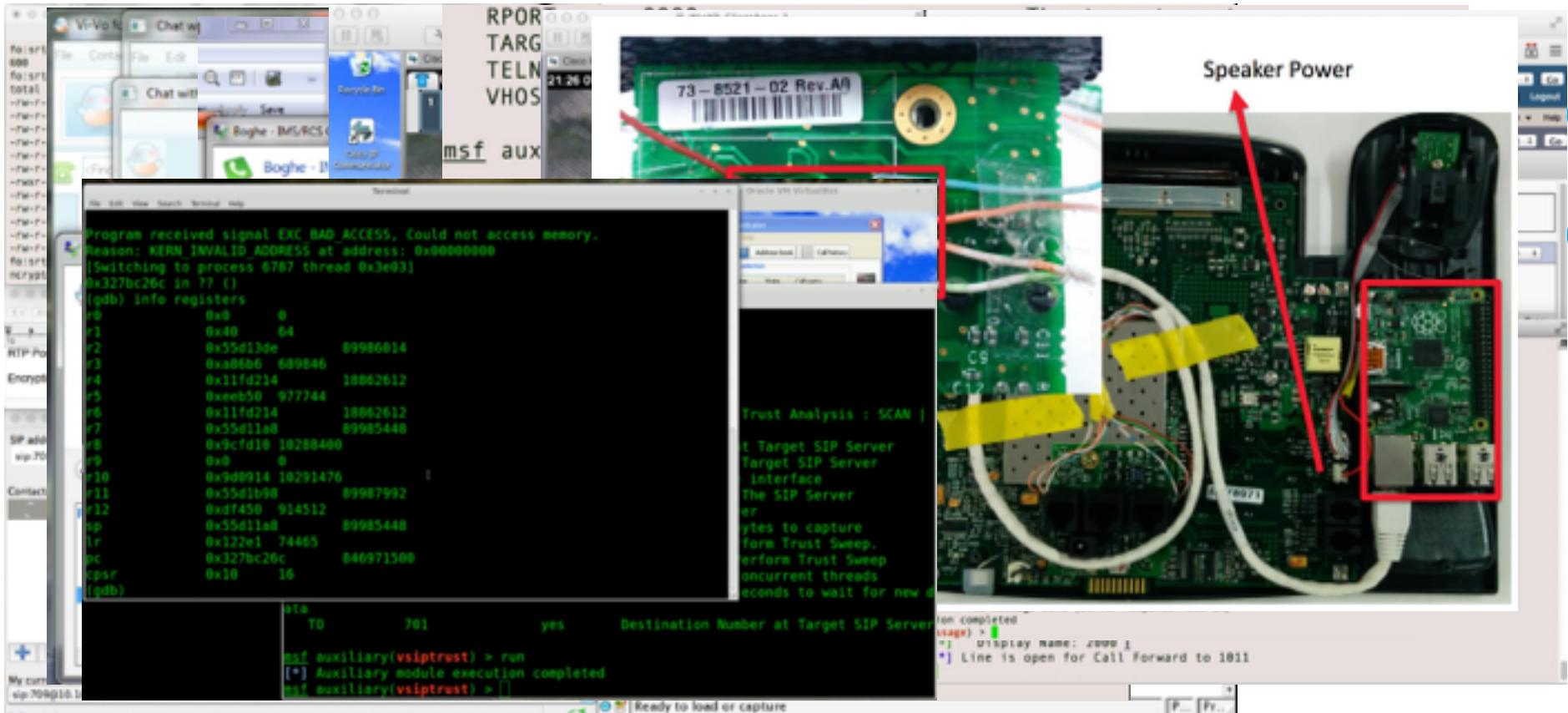
www.senseofsecurity.com.au  
ABN: 14 098 237 908



# Fatih Ozavci, Principal Security Consultant

- VoIP & phreaking
- Mobile applications and devices
- Network infrastructure
- CPE, hardware and IoT hacking
- Author of Viproxy, Viproxy and VoIP Wars research series
- Public speaker and trainer  
Blackhat USA, Defcon, HITB, AusCert, Troopers, Ruxcon

# Previously on VoIP Wars



- This is only the first stage of the research
  - Analysing the security requirements of various designs
  - Developing a tool to
    - assess communication and voice policies in use
    - drive official client to attack other clients and servers
    - debug communication for further attacks
- Watch this space
  - Viproxy with Skype for Business authentication support
  - Potential vulnerabilities to be released

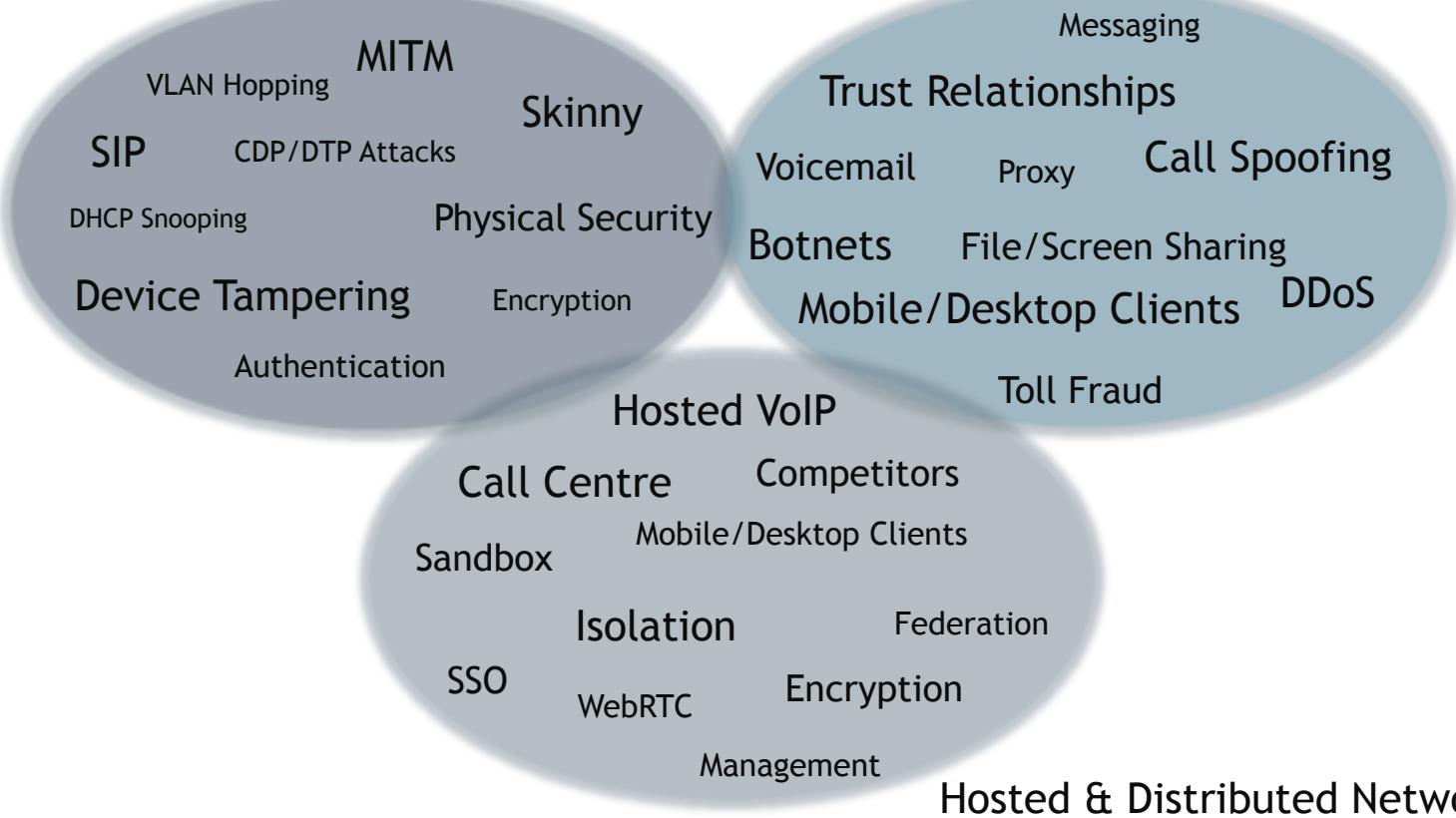


1. Modern threats targeting UC on Skype for Business
2. Security requirements for various implementations
3. Security testing using Viproxy
4. Demonstration of vulnerabilities identified

# Security requirements for UC

## Corporate Communication

## Commercial Services



## Voice hackers' legal career 'hit by

the guardian

IT News | World | Sport | Comment | Culture | Business | Environment

News | UK news

Phone hacking may have led to Milly Dowler voicemail deletions, says judge  
Voice messages, once hacked, would have been deleted automatically, Mr Justice Saunders tells Old Bailey jury

Lisa O'Carroll  
[TheGuardian.com](#), Friday 6 June 2014 05.12 AEST



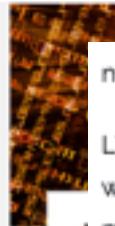
Credit: Stuart Fullerton sounded like a headteacher, according to a member of staff from Monday's Agency... (the court heard). Photograph: Mark Thomas/PA Features  
Re: Murdered schoolgirl Milly Dowler's voicemails would have been deleted automatically after they were hacked by the News of the World, the Old Bailey heard.  
Im: authentication

26 Jul 2015 at 11:22, Simon Rockman

A new VoIP service allows you to hide who you are by being web-allowed you to spoof caller identity, and pay by Bitcoin.

nd Ben Carter  
toney Box

The  
ComputerWeekly.com



ZDNet



CLOUD CXO SMB STORAGE HARDWARE INNOVATION MOBILITY MORE NEWSLETTERS

REVIEW MICROSOFT SURFACE BOOK: A NICE LAPTOP, BUT STILL NOT MY 'ULTIMATE' PC

## 'All Android devices' vulnerable to new LTE security flaw

network.'

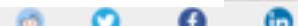
LTE (also known as 4G) relies on packet switching, a common way of sending data across the internet, rather than the old method of circuit switching. This new method of sending data allows for new kinds of attacks, particularly against the Session Initiation Protocol (SIP), nowadays more commonly used in voice calls and instant messaging.

Researchers have found a method that exploits the way that SIP works, by spoofing phone numbers for calls or text messages. It's also possible for an attacker to obtain free bandwidth for more data-intensive activities, like video calling, without incurring any additional costs. In some cases, an attacker can establish multiple SIP sessions at the same time, which could lead to a denial-of-service attack on the network.

The latest round of vulnerabilities affects potentially every Android device, say researchers.

[Read More](#)

24 Apr 2014 at 12:34, Simon Rockman





**hotmail**

Microsoft Live  
Communications  
2005

Microsoft Office  
Communicator  
2007

Microsoft Lync  
2000 - 2013

Microsoft Skype for  
Business 2015



- Active Directory, DNS (SRV, NAPTR/Enum) and SSO
- Extensions to the traditional protocols
  - SIP/SIPE, XMPP, OWA/Exchange
  - PSTN mapping to users
  - Device support for IP phones and teleconference systems
  - Mobile services
- Not only for corporate communication
  - Call centres, hosted Lync/Skype services
  - Office 365 online services, federated services





Client A

↑  
SRTP  
(AES)  
↓

RTP  
Proxy

1- REGISTER

1- 200 OK

2- INVITE

2- 100 Trying

4- 200 OK

4- ACK



Skype for Business 2015

3- INVITE

3- 200 OK



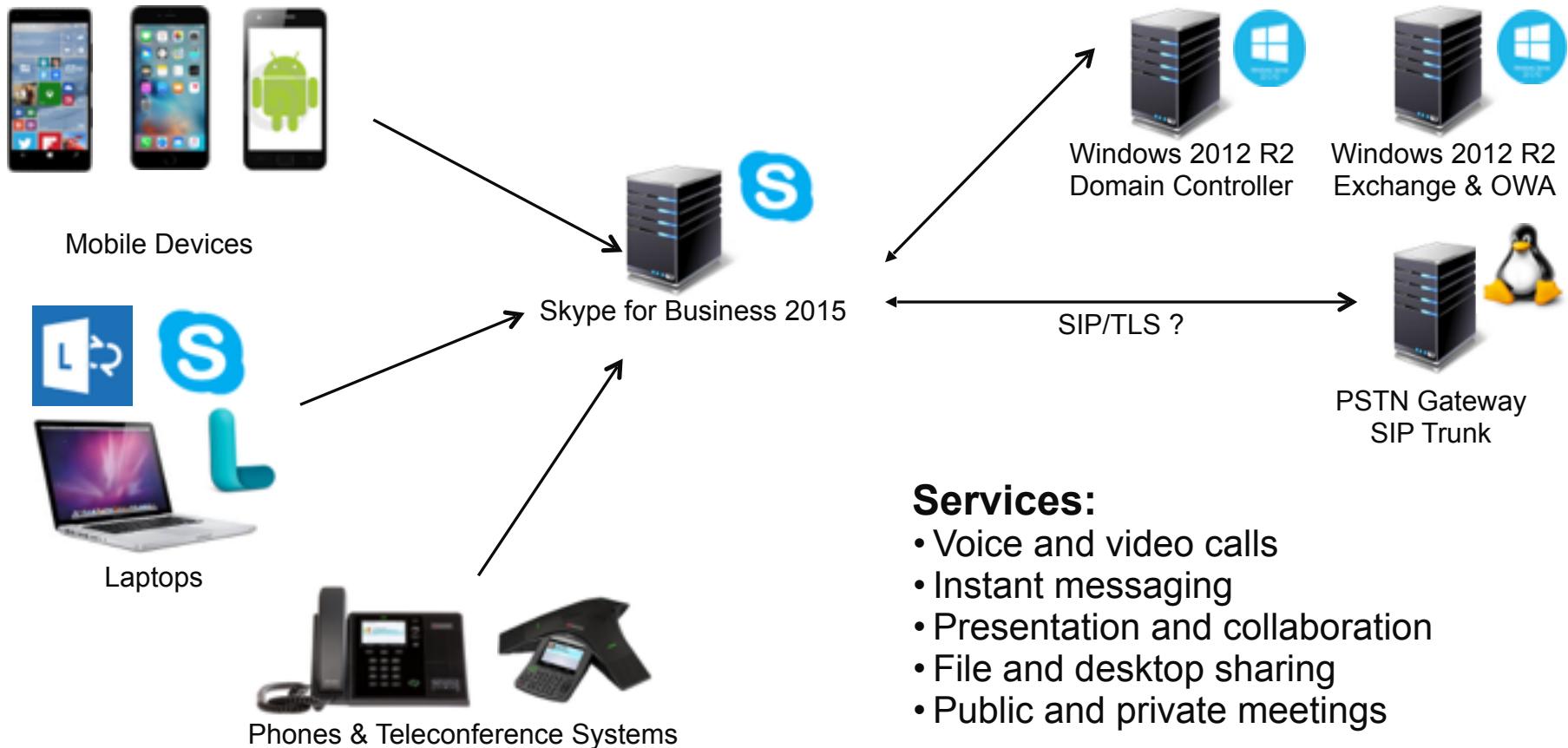
Client B

SRTP (AES)

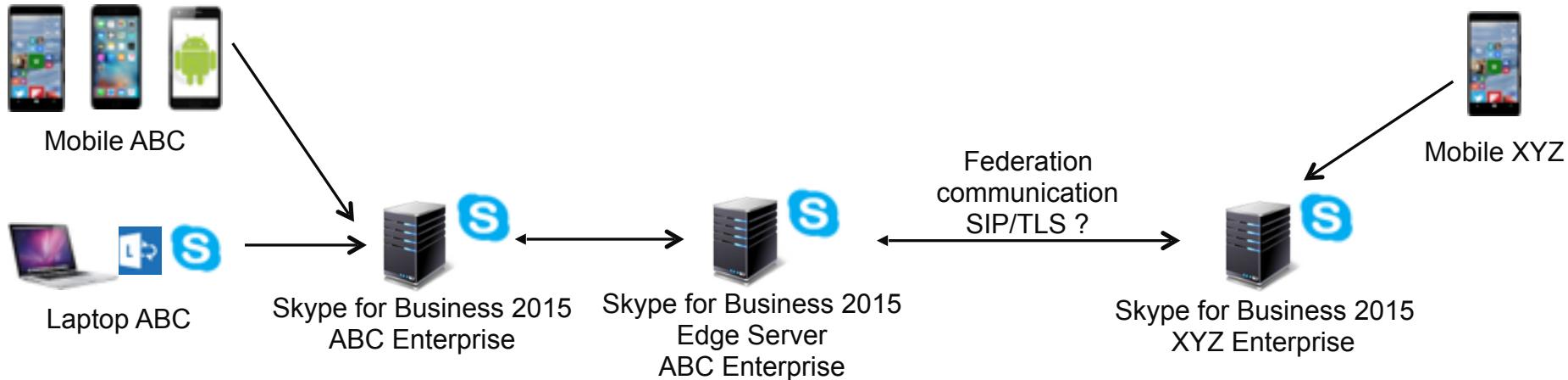
SRTP (AES)

SRTP (AES)

# Corporate communication



# Federated communication



DNS Server

## Services:

- Federation connections (DNS, Enum, SIP proxies)
- Skype for Business external authentication
- Connecting the users without individual setup
- Public meetings, calls and instant messaging

# Supported client features

Feature/capability	Skype for Business	Skype for Business Web App	Lync 2013	Lync Windows Store app	Lync 2013 Basic	Lync 2010	Lync 2010 Attendant	Lync Phone Edition	Communicator for Mac 2011	Lync for Mac 2011
Initiate IM with a public contact	•		•	•	•	•	• <sup>1</sup>		•	•
Initiate IM with a federated contact	•		•	•	•	•	• <sup>1</sup>		•	•
Conduct two-party or multiparty calls with external users	• <sup>2</sup>		• <sup>2</sup>	• <sup>2</sup>	•	•	• <sup>1</sup>	•	•	•

<sup>1</sup>Lync 2010 Attendant is not supported in Skype for Business Online and Office 365.

<sup>2</sup> This feature is not available in Skype for Business Online and Office 365.

# Supported client features

Give control?

Give control?

Feature/capability	Skype for Business	Skype for Business Web App	Lync 2013	Lync Windows Store app	Lync 2013 Basic	Lync 2010	Lync 2010 Attendant	Lync Phone Edition	Communicator for Mac 2011	Lync for Mac 2011
Participate in multiparty IM	•	•	•	•	•	•	• <sup>1</sup>		•	•
Share the desktop (if enabled)	•	• (requires plug-in)	•		•				• <sup>2</sup>	• <sup>2</sup>
Share a program (if enabled)	•	• (requires plug-in)	•		•					View only
Add anonymous participants (if enabled)	•	•	•		•					•
Use dial-in audio conferencing	• <sup>3</sup>	• <sup>3</sup>	• <sup>3</sup>	• <sup>3</sup>	• <sup>3</sup>	•	• <sup>1</sup>			•
Initiate a Meet Now meeting	•		•	•	•					•

<https://technet.microsoft.com/en-au/library/dn933896.aspx>

- SIP over TLS is enforced for clients by default
- SRTP using AES is enforced for clients by default
- SIP replay attack protections are used on servers
  - Responses have a signature of the critical SIP headers
  - Content itself and custom headers are not in scope
- Clients validate the server response signatures
- SIP trunks (PSTN gateway) security
  - TLS enabled and IP restricted
  - No authentication support



- Defcon 20 - The end of the PSTN as you know it
  - Jason Ostrom, William Borskey, Karl Feinauer
  - Federation fundamentals, Enumerator, Lyncspoof
- Remote command execution through vulnerabilities on the font and graphics libraries (MS15-080, MS15-044)
- Targeting Microsoft Lync users with malwared Microsoft Office files
- Denial of service and XSS vulnerabilities (MS14-055)

- 3 ways to conduct security testing
  - Compliance and configuration analysis
  - MITM analysis (Viproxy 2.0)
  - Using a custom security tester (Viproxy 4.0 is coming soon)
- Areas to focus on
  - Identifying design, authentication and authorisation issues
  - Unlocking client restrictions to bypass policies
  - Identifying client and server vulnerabilities
  - Testing business logic issues, dial plans and user rights

- Autodiscovery features
  - Autodiscovery web services
  - Subdomains and DNS records (SRV, NAPTR)
- Web services
  - Authentication, Webtickets and TLS web services
  - Meeting invitations and components
  - Skype for Business web application
- Active Directory integration
- Information gathering via server errors



- Design of the communication infrastructure
  - Phone numbers, SIP URIs, domains, federations, gateways
- Client type, version and feature enforcements
  - Meeting codes, security, user rights to create meetings
  - Open components such as Skype for Business web app
  - Feature restrictions on clients
  - File, content and desktop sharing restrictions
- User rights (admin vs user)
- Encryption design for signalling and media



**Skype for Business Server**

- Home
- Users
- Topology
- IM and Presence
- Persistent Chat
- Voice
  - Home
  - Users
  - Topology
  - IM and Presence
  - Persistent Chat
  - Voice Routing
  - Voice Features
  - Response Groups
  - Conferencing
  - Clients
  - Federation and External Access
  - Monitoring and Archiving
  - Security
  - Network Configuration
- Associated PSTN Usages
  - New
  - Select...
  - Remove
- PSTN usage record
- Long Distance
- Internal

CONFERENCE POLICY MEETING CONFIGURATION DIAL-IN ACC

Edit Conferencing Policy - Global

Allow multiple

**Commit** **Cancel**

The default/custom policies should be assigned to users and groups

**Skype for Business Server**

EXTERNAL ACCESS POLICY

Home Users Topology

Edit External Access

**IM and Presence**

**Commit**

Scope: Global Name: \*

Description: Global

Enable com

Enable com users

Enable com

Enable com communications with public users

FILE FILTER URL FILTER

Edit URI Filter - Global

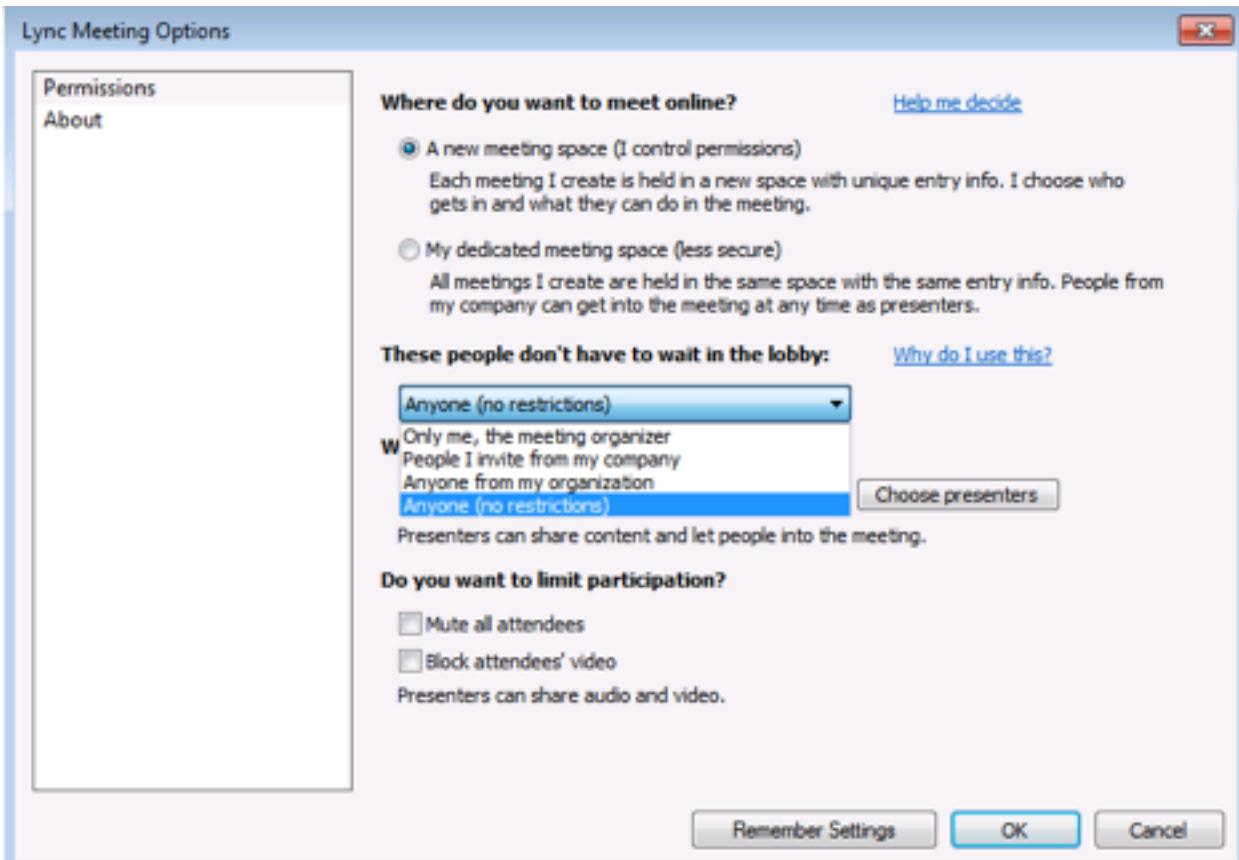
**Commit** **Cancel**

Scope: Name: Global

IM and Presence Persistent Chat Voice Routing Voice Features Response Groups Conferencing Clients Federation and External Access Monitoring and Archiving Security Network Configuration

**New** **Show details...** **Remove** **Up** **Down**

User agent	Version	Operation	Action
HC	14.0.*.*	Older than	Block
RTC	1.3.*.*	Older than or same as	Allow
WM	1.5.*.*	Older than or same as	Allow
OC	3.5.4907.233	Older than	Block
OC	3.999.9999.9999	Older than or same as	Allow
QC	4.0.7977.4600	Older than	Allow
QC	4.999.9999.9999	Older than or same as	Allow
QC	15.0.4128.0	Older than	Allow
MOOP	2.8.5999.*	Older than or same as	Block



- Meeting rights to be assigned by users
- Policies assigned are in use



- SRTP using AES is enforced for clients (No ZRTP)
- SIP/TLS is enforced for clients
- SIP/TLS is optional for SIP trunks and PSTN gateways
  - Compatibility challenges vs Default configuration
  - SIP/TCP gateways may leak the SRTP encryption keys

a=ice-ufrag:x30M

a=ice-pwd:oW7iYHXiAOr19UH05ba07bMJ

a=crypto:2 **AES\_CM\_128\_HMAC\_SHA1\_80** inline:Gu  
+c81XctWoAHro7cJ9uN6WqW7QPJndjXfZsof18|2^31|1:1

- Challenges
  - SIP/TLS is enabled by default
  - Microsoft Lync clients validate the TLS cert
  - Compression is enabled, not easy to read
- Viproxy 2.0
  - A standalone Metasploit module
  - Supports TCP/TLS interception with TLS certs
  - Disables compression
  - Modifies the actions of an official client
  - Provides a command console for real-time attacks



- Debugging the protocol and collecting samples
- Basic find & replace with fuzzing support
- Unlocking restricted client features
- Bypassing communication policies in use
- Injecting malicious content



MS Lync for Mac 2011  
Client to be used for attacks



Viproxy 2.0



Windows 10  
Skype for Business Clients

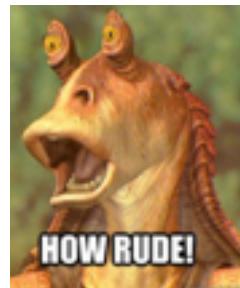


Windows 2012 R2  
Skype for Business 2015 Server

- Instant Messaging (IM) restrictions
  - File type filters for the file transfers
  - URL filters for the messaging
  - Set-CsClientPolicy (DisableEmoticons, DisableHtmlIm, DisableRTFIm)
- Call forwarding rights
- Meeting rights
  - Federated attendees
  - Public attendees
  - Clients' default meeting settings
- Insecure client versions allowed



- Various content types (HTML, JavaScript, PPTs)
- File, desktop and presentation sharing
- Limited filtering options (IIMFilter)
  - File Filter (e.g. exe, xls, ppt, psh)
  - URL Filter (e.g. WWW, HTTP, call, SIP)
  - Set-CsClientPolicy (DisableHtmlIm, DisableRTFIm)
- Clients process the content before invitation
  - Presence and update messages
  - Call and IM invitation requests
  - Mass compromise via meetings and multiple endpoints



- Custom SIP extensions
- XML based INVITE and SUBSCRIBE content
- HTML/ Javascript based messaging (IM)
- Instant and unusual disconnects
- C# and C++ combination for apps
- File and desktop sharing through RTP sessions



# Parsing errors and exceptions

Warning ModLoad: 00007ffe`98a90000 00007ffe`98a9c000 C:\Windows\SYSTEM32\asacm32.drv  
ModLoad: 00007ffe`98490000 00007ffe`9849a000 C:\Windows\SYSTEM32\midimap.dll  
Info: trace-currentCall=10: 000154/502  
Info: Instance-Id: 2C7  
Info: Direction: outgoing;source="local"  
TL\_ERROR Peer: 192.168.2.111:50421  
(Apimodu Message-Type: request  
Returned Start-Line: BEMNOTIFY sip:192.168.2.111:50421;transport=tls;ms-opaque=a42a3baef4;ms-received-cid=7500;grid  
TL\_ERROR SIP/2.0  
(Apimodu From: <sip:test1@lync2012.com>;tag=3E0F0080  
Returned To: <sip:test1@lync2012.com>;tag=04917900f3;epid=76d2784be7  
TL\_ERROR Call-ID: 6c613c61b864194e888f418c2a76d13a  
(Apimodu CSeq: 3 BEMNOTIFY  
0xC3E93FVia: SIP/2.0/TLS 192.168.103.103:5061;branch=z9hG4bKB4944566.7EE067DFAC06526E;branched=FALSE  
TL\_WARN Max-Forwards: 70  
(Apimodu Content-Length: 4115  
Reply w/Content-Type: application/  
TL\_WARN Message-Body: ----\*\*\*\*\*MESSAGE BODY DELETED\*\*\*\*\*----  
[3983509  
TL\_ERROR TL\_ERROR(TF\_COMPONENT) [lync\lync]1908.23CC::09/11/2015-07:10:22.592.0000FCDC  
(Apimodu (UserServices,CSubscribe ) [2230686419]( 00000041234723E0 ) Xm  
[0000004 parser returned an error [hr=HRESULT=C00CEE01] Returned HRESULT=C00CEE01  
TL\_INFO TL\_ERROR(TF\_COMPONENT) [lync\lync]1908.23CC::09/11/2015-07:10:22.592.0000FCDD  
(Apimodu (UserServices,CSubscribe ) [2230686419]( 00000041234723E0 ) Xm  
Cause: parsing failed: [Unexpected end of input.  
Resolution: 00000041234723E0  
Contact: 00000041234723E0  
TL\_ERROR(TF\_COMPONENT) [lync\lync]1908.23CC::09/11/2015-07:10:22.592.0000FCDE  
(Apimodu (UserServices,CCategoriesSub ) .cpp(146)) [2230686419](

# CVE-2015-6061 (MS15-123)

## Impact:

- Unauthorised script execution
- Security bypass

## Microsoft Security Bulletin MS15-123 – Important

24 out of 32 rated this helpful – [Rate this topic](#)

### Security Update for Skype for Business and Microsoft Lync to Address Information Disclosure (3105872)

Published: November 10, 2015

Version: 1.0

#### Executive Summary

This security update resolves a vulnerability in Skype for Business and Microsoft Lync. The vulnerability could allow information disclosure if an attacker invites a target user to an instant message session and then sends that user a message containing specially crafted JavaScript content.

This security update is rated important for all supported editions of Skype for Business 2016, Microsoft Lync 2013, and Microsoft Lync 2010; it is also rated important for certain Microsoft Lync Room System components. For more information, see the [Affected Software](#) section.

#### On this page

[Executive Summary](#)

[Affected Software](#)

[Update FAQ](#)

[Vulnerability Information](#)

[Security Update Deployment](#)

[Acknowledgments](#)

[Disclaimer](#)

[Revisions](#)

Bulletin ID	Vulnerability Title	CVE ID	Exploitability Assessment for Latest Software Release	Exploitability Assessment for Older Software Release	Denial of Service Exploitability Assessment
MS15-123	Server Input Validation Information Disclosure Vulnerability	CVE-2015-6061	2 – Exploitation Less Likely	2 – Exploitation Less Likely	Not Applicable

<https://technet.microsoft.com/en-us/library/security/ms15-123.aspx>  
<https://support.microsoft.com/en-us/kb/3105872>

IM URL filter for Microsoft Skype for Business 2015 (Microsoft Lync 2013) server can be bypassed with content obfuscation

```
<script>var u1="ht"; u2="tp"; u3="://" ;o="w"; k="."; i="";
u4=i.concat(o,o,o,k);
window.location=u1+u2+u3+u4+"senseofsecurity.com"</script>
```



Reverse browser visiting

Windows 10  
Skype for Business ClientMS Lync for Mac 2011  
Client to be used for attacking

Malicious MESSAGE



Viproxy 2.0

Windows 2012 R2  
Skype for Business 2015 Server

SFB Client1

Recycle Bin

Skype for Business

What's happening today?

test12 Available Set Your Location

Find someone or dial a number

GROUPS STATUS RELATIONSHIPS NEW

Favorites

john doe - Offline 4 days

test3 - Offline

+102

100

test1 - Available - Video Capable Available

OTHER CONTACTS (0)

CALL FORWARDING OFF

1:40 PM  
29/08/2015

metasploit-framework-with-viproy — ruby — 97x14

msf auxiliary(viproy\_volp\_mitm) > jobs

Jobs

msf auxiliary(viproy\_volp\_mitm) >

Id Name

-- ----

13 Auxiliary: volp/viproy\_volp\_mitm

msf auxiliary(viproy\_volp\_mitm) >

Microsoft Lync

test1 Available Set Your Location

available

Contacts Phone History

Find a contact or dial a number

Pinned Contacts (0)

john doe - Offline

test3 - Offline

Other Contacts (1/1)

test2 - Available

Test2

test2 - Available

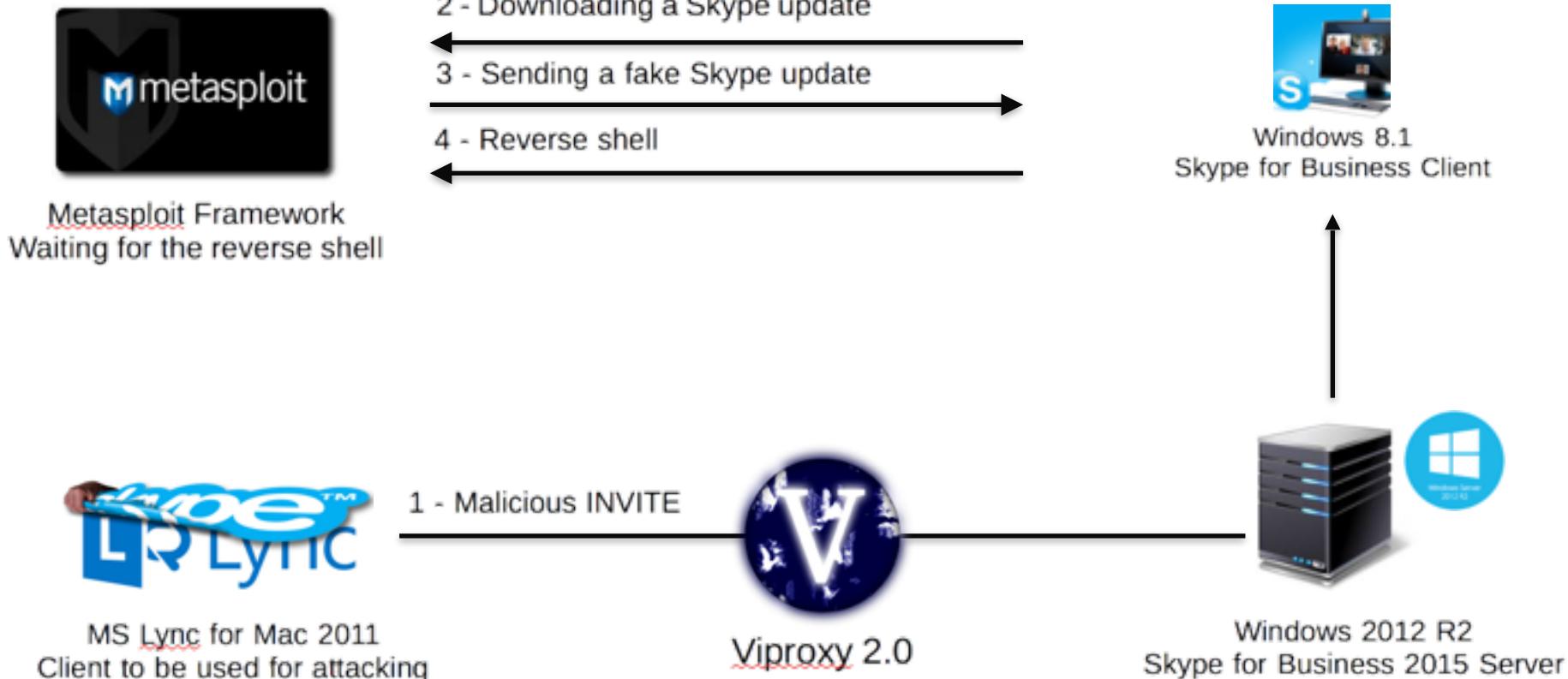
Microsoft Skype for Business 2015 (Microsoft Lync 2013) client executes HTML and JavaScript content in the SIP INVITE request headers without user interaction

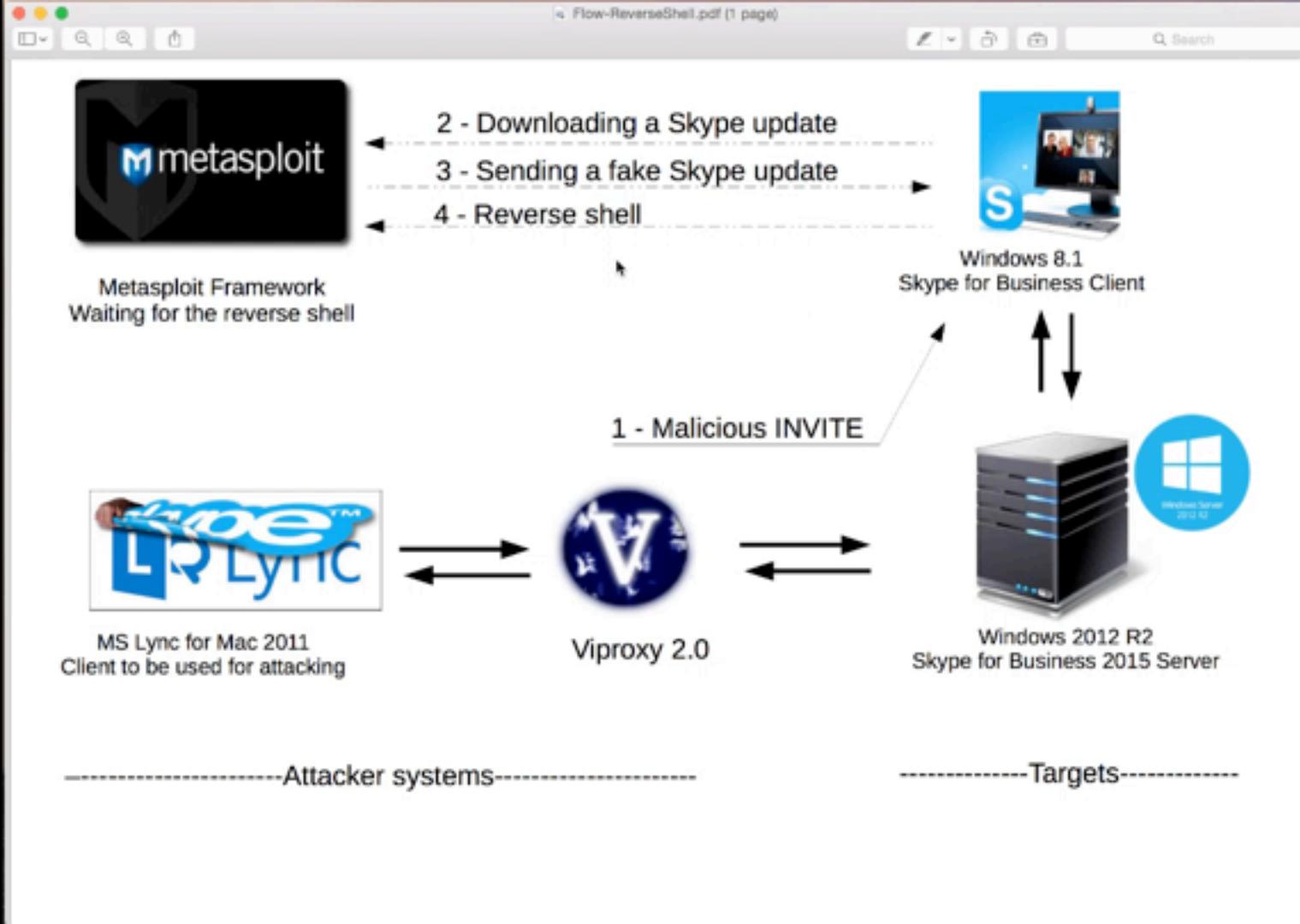
- No user interaction required

Ms-IM-Format: text/html; charset=UTF-8; ms-body=PHNjcmlwdD53aW5kb3cubG9jYXRpb249Imh0dHA6Ly93d3cuc2Vuc2VvZnNlY3VyaXR5LmNvbS5hdSI8L3NjcmllwdD4K

Base64 decode: <script>window.location="http://www.senseofsecurity.com.au"</script>

# Fake Skype update via INVITE





- Meeting requests
  - Private meetings, Open meetings, Web sessions
- Multi callee invitations and messages
  - Attacks do not need actions from the attendees/callees
- Injecting endpoints to the requests
  - XML conference definitions in the INVITE requests
  - INVITE headers
  - Endpoint headers
- 3<sup>rd</sup> party SIP trunk, PSTN gateway or federation

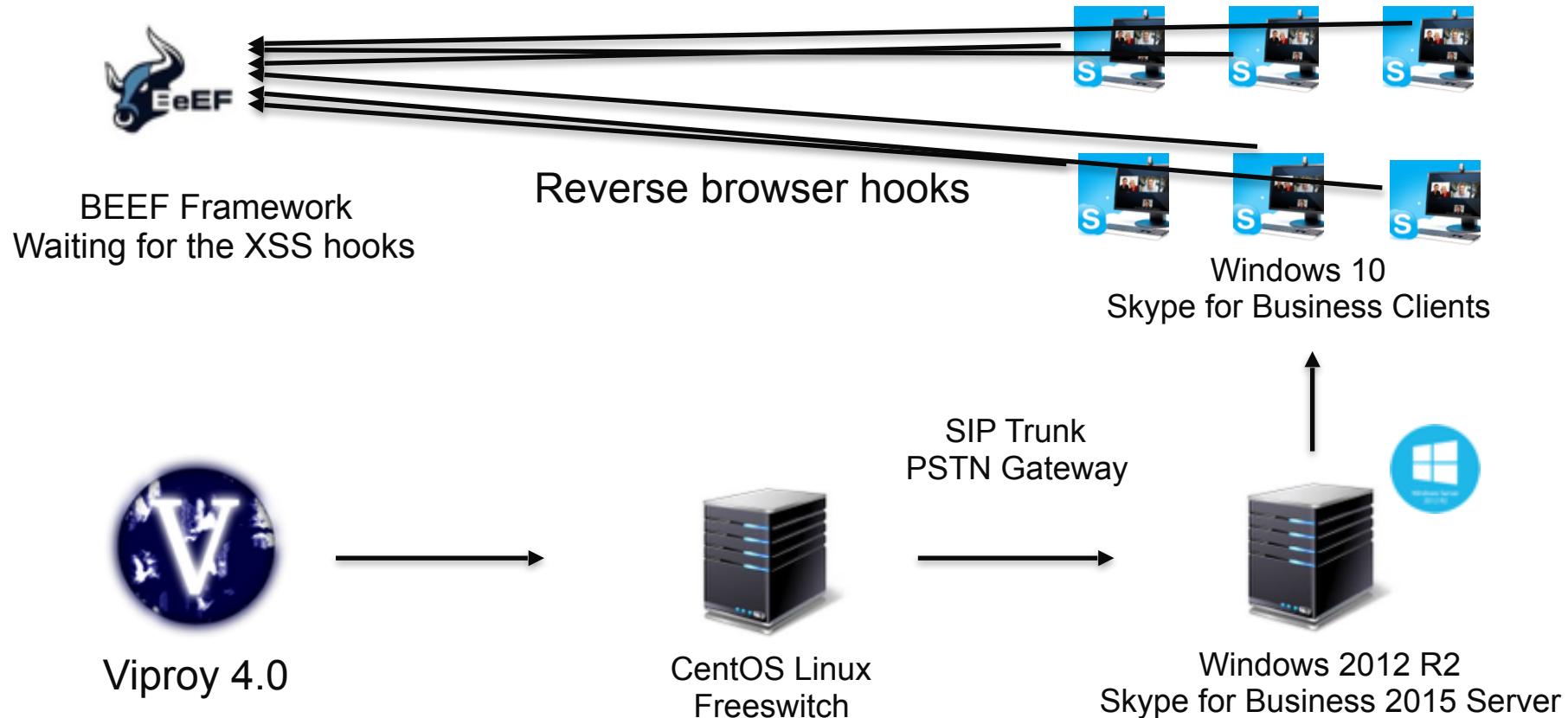
Microsoft Skype for Business 2015 (Microsoft Lync 2013) client executes HTML and JavaScript content in the SIP MESSAGE requests without user interaction

- No user interaction required

Content-type: text/html

```
<script>window.location="http://  
www.senseofsecurity.com.au"</script>
```

# Mass compromise of clients



# Mass compromise of clients



- 2 – Requesting the Browser Autopwn page
- 3 – Sending a bunch of exploits
- 4 – Reverse shells



Windows 7   Windows 8.1  
Skype for Business Clients



MS Lync for Mac 2011  
Client to be used for attacking

- 1 - Malicious MESSAGE

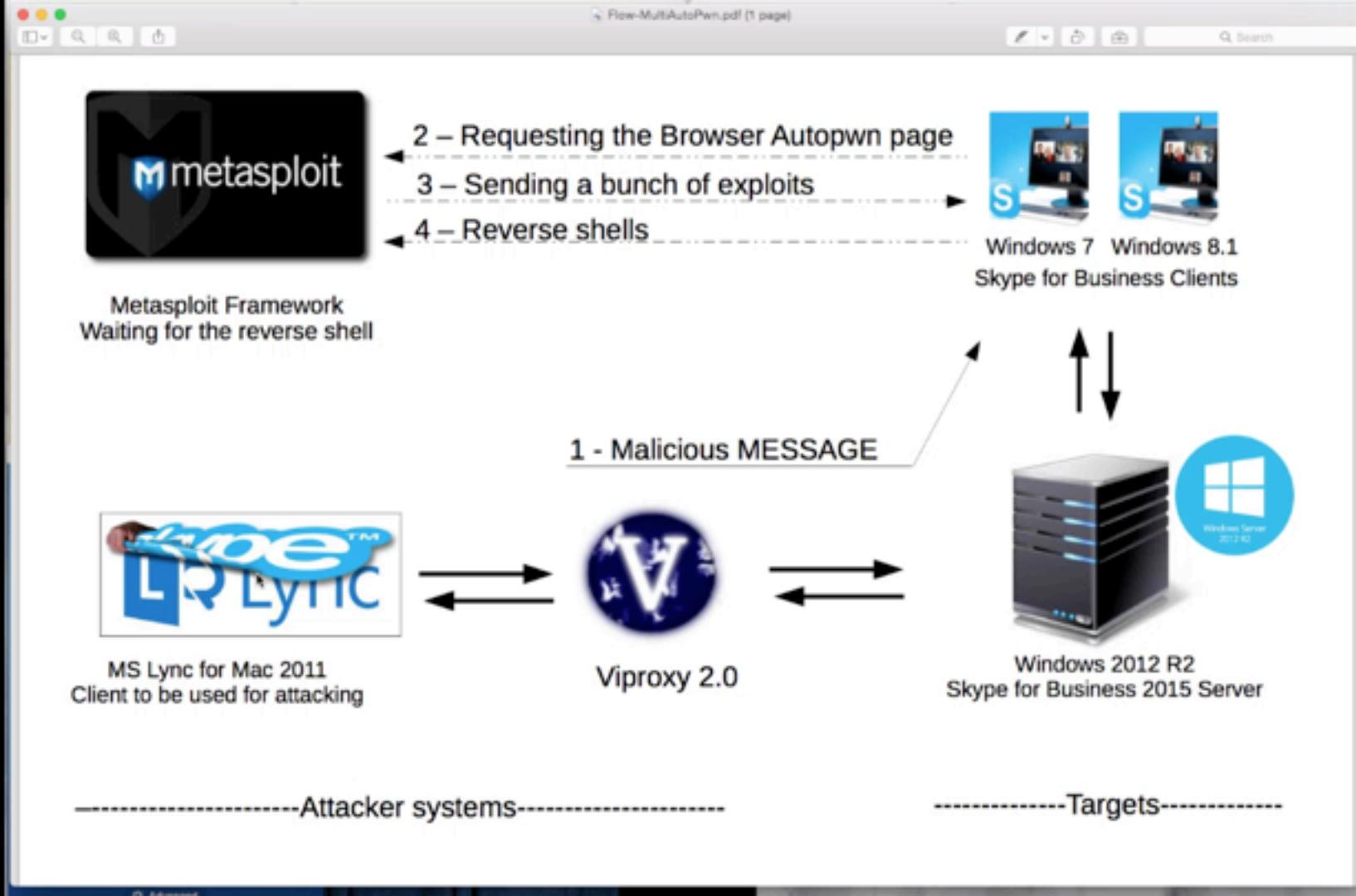


Viproxy 2.0



Windows 2012 R2  
Skype for Business 2015 Server





## Analysis of

- mobile clients and SFB web app
- SFB meeting security and public access
- federation security and trust analysis
- Further analysis of the crashes and parsing errors identified for exploitation
- Social engineering templates for Viproxy and Viproy
- Viproy 4.0 with Skype for Business authentication, fuzzing and discovery support

Secure design is always the foundation

- Physical security of endpoints (e.g. IP phones, teleconference rooms) should be improved
- Networks should be segmented based on their trust level
- Authentication and encryption should be enabled
- Protocol vulnerabilities can be fixed with secure design
- Disable unnecessary IM, call and meeting features
- Software updates should be reviewed and installed

- Microsoft Skype for Business 2015 is the next-generation Unified Communications system, though it still has legacy vulnerabilities and design issues.
- There are new security testing tools to test it with new vulnerabilities and techniques which are Viproxy and Viproy.
- Secure design is the foundation for securing Unified Communications, and it reduces the attack surfaces.

## VoIP Wars I: Return of the SIP (Defcon, Cluecon, Ruxcon, Athcon)

- Modern VoIP attacks via SIP services explained
- SIP trust hacking, SIP proxy bounce attack and attacking mobile VoIP clients demonstrated
- <https://youtu.be/d6cGlTB6qKw>

## VoIP Wars II : Attack of the Cisco phones (Defcon, Blackhat USA)

- 30+ Cisco HCS vulnerabilities including 0days
- Viproy 2.0 with CUCDM exploits, CDP and Skinny support
- Hosted VoIP security risks and existing threats discussed
- <https://youtu.be/hqL25srtoEY>

## The Art of VoIP Hacking Workshop (Defcon, Troopers, AusCERT, Kiwicon)

- Live exploitation exercises for several VoIP vulnerabilities
- 3 0day exploits for Vi-vo and Boghe VoIP clients
- New Viproy 3.7 modules and improved features
- <https://www.linkedin.com/pulse/art-voip-hacking-workshop-materials-fatih-ozavci>

## Viproxy VoIP Penetration and Exploitation Kit

Author : <http://viproxy.com/fozavci>

Homepage : <http://viproxy.com>

Github : <http://www.github.com/fozavci/viproxy-voipkit>

## VoIP Wars : Attack of the Cisco Phones

<https://youtu.be/hqL25srtoEY>

## VoIP Wars : Return of the SIP

<https://youtu.be/d6cGlTB6qKw>



<https://www.senseofsecurity.com.au/aboutus/careers>

# Questions



# Thank you

Head office is level 8, 66 King Street, Sydney, NSW 2000, Australia.  
Owner of trademark and all copyright is Sense of Security Pty Ltd.  
Neither text or images can be reproduced without written  
permission.

T: 1300 922 923  
T: +61 (0) 2 9290 4444  
F: +61 (0) 2 9290 4455  
[info@senseofsecurity.com.au](mailto:info@senseofsecurity.com.au)  
[www.senseofsecurity.com.au](http://www.senseofsecurity.com.au)